DOD Privacy Impact Assessment (PIA)

1. DA organizational name (APMS Sub Organization name).

U.S. Army, Office of the Assistant G-1 for Civilian Personnel

2. Name of Information Technology (IT) System.

Civilian Human Resource Activity Based Costing System (CHR-ABC)

3. Budget System Identification Number (SNAP-IT Initiative Number).

N/A

4. System Identification Numbers(s) (IT Registry/Defense IT Portfolio Repository (DITPR)).

2795

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable).

N/A

6. Privacy Act System of Records Notice Identifier (if applicable).

A0690-200 DAPE, Department of the Army Civilian Personnel Systems

7. OMB Information Collection Requirement Number (if applicable) and Expiration Date.

N/A

8. Type of authority to collect information (statutory or otherwise).

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 3013, Secretary of the Army
Army Regulation 690-200, General Personnel Provisions
Executive Order 9397

9. Provide a brief summary or overview of the IT system (activity/purpose, present lifecycle phase, system owner, system boundaries and interconnections, location of the system and components, and system backup)

The CHR-ABC Data Entry system is a web application that enables civilian personnel to record their work time against a list of functions and key activities. Users enter their

time through Daily and Weekly View screens and this information is then integrated with payroll data and overhead costs where it is then analyzed to determine the cost of the various functions and activities. CHR ABC is an existing system that is in the development process life cycle phase. The system contains information pertaining to Army civilian workforce personnel.

CHR ABC operates within the Army Civilian Personnel Data System (ACPDS), which operates as part of the Army's Active Directory (AD) implementation. The ACPDS is connected to the DoD Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) via the installation backbone. Personal computer-to-server and server-to-server connections are protected by an encryption tool for servers and the Windows Operating System. Data transferred is also protected by encryption. Users access CHR-ABC via an Army accredited Microsoft Internet Explorer Client using Secure Socket Layer (SSL) encryption. Web servers and database servers are located at the Army Civilian Data Center (ACDC) in Rock, Island Illinois.

The CHR ABC system is backed up via daily tape backups. Tapes are maintained up to six months at the Army Civilian Data Center.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g. names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.)

Information in identifiable form that is collected includes: name, social security number, date of birth, hours worked, duty status, salary, pay grade, title, residence allowance, housing allowance and lunch allowance. Information used by CHR ABC is extracted from DCPDS through a secure server via an encrypted network.

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).

Basic identity information used by CHR ABC is extracted from DCPDS through a secure server via an encrypted network. Individuals enter their own time and attendance information through a web-based application.

12. Describe the requirement and why the information in identifiable for is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc.).

This system allows the Army to properly track and record working time spent by civilian personnel in the accomplishment of official duties. This system ensures proper tracking of labor and compensation expenditures. Information in identifiable form is collected and used by this system in direct support of these missions.

13. Describe how the information in identifiable form will be used (e.g. to verify exiting data, etc.).

Information in identifiable form entered into the system is used to produce reports that will help justify and document the efficiency and effectiveness of Army CHR professionals.

14. Describe whether the system derives or creates new data about individuals through aggregation.

This system does not derive or create new information about individuals through aggregation.

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.).

Information will be available to authorized users with a need to know in order to perform official government duties. Information from this system is shared among the Army personnel community which consists of the Civilian Personnel Operations Centers, the Civilian Personnel Advisory Centers, Army Civilian Human Resources Agencies and U.S. Army Garrisons at installations and Headquarters, U.S. Army Installation Management Command. Other internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include Department of Defense Inspector General, Defense Manpower Data Center, Defense Criminal Investigative Service, Under Secretary of Defense for Personnel & Readiness, Army Staff Principals in the chain of command, Department of Army Inspector General, Army Audit Agency, US Army Criminal Investigative Command, US Army Intelligence and Security Command, Provost Marshal General and Assistant Secretary of the Army for Financial Management and Comptroller. In addition, the DoD blanket routine uses apply to this system.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable for about themselves or to contest to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

Basic identity information used by CHR ABC is extracted from DCPDS through a secure server via an encrypted network. Individual record subjects are not involved in this process. Individuals give implied consent to the use, collection and storage of their personally identifiable information when they initially provide information to Army civilian personnel systems. Individuals enter their own time and attendance information into the system via a web-based application at which time privacy advisories are displayed.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of the delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

A Privacy Act statement in electronic form describing the use, dissemination and collection of information in identifiable form is located on the web site where users enter their information.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

This system has a current certification and accreditation. The system resides on a secure military installation within secure facilities. These facilities have armed guards that verify the credentials (appropriate DoD building/identification badge) of all employees and login all visitors including, vendors and maintenance. Cameras are also used to monitor activity around the installation. Additionally, the system is built on redundancy with a full Continuity of Operations site. System users include Army Civilian and contract Personnel under the administrative control of the Civilian Information Services Division (CISD). Personnel with system administration privileges are required to have background investigations at the Automatic Data Processing / Information Technology (ADP/IT) I or II level and to sign a non-disclosure agreement. All personnel accessing government computer information are required to have a minimum of ADP/IT III background investigation.

Users may have access requirements and are limited to specific or general information in the computing environment. The system administrator defines specific access requirements dependent upon each user's role. Each specific application in the system may further restrict access via application-unique permission controls. Users must enter appropriate user Identification and password before being authorized access to the resources. A user's manual was designed to fulfill the needs of the different types of employees (e.g., users, administrators, managers, etc.). Additionally, all aspects of privacy, security, configuration, operations, data retention and disposal are documented to ensure privacy and security are consistently enforced and maintained. There is weekly monitoring of security events, network intrusion detection, firewall and regular adherence to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIGs). Files transferred across the internet/NIPRNET are encrypted.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program", November 11, 2004. If so, and a System of Records Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when the publication of the notice will occur.

This system requires a SORN and it is published.

20. Describe/evaluate any potential privacy risk regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate and privacy risks in providing individuals and opportunity to object/contest or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

Safeguards are employed to detect and minimize unauthorized disclosure, modification, and/or destruction of data thus we believe the risk to the individual's privacy to be minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals. Risks are further mitigated by the implementation of firewalls, intrusion detection systems and malicious code protection

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

The data in the system is For Official Use Only. The PIA may be published in full.